DS PRIVACY POLICY AND PROCEDURE

drummond street services
wellbeing for life

Stepfamilies Australia
Strengthening Stepfamilies

queerspace
our health in our hands

CFRE
Centre for
FAMILY RESEARCH
and EVALUATION

the drum
YOUTH SERVICES

We acknowledge the traditional owners of the land where we work and pay respects to elders past, present and future.

OVERVIEW

drummond street services (**ds**) provides a range of support services to many clients each year. By definition, the client information **ds** collects, holds, and shares, when required is sensitive and personal. This policy sets out how **ds** delivers on its legal and ethical obligations to protect privacy so that **ds** can:

» Enacts its commitment to privacy, through clear explanations and information on how it ensures and meets its privacy obligations

» promote greater public confidence in the organisation's handling of personal information

» help all **ds** staff , including students, volunteers, and across all levels of the organisation understand and provide guidance how they must handle the personal information they collect, and

» prevent the unnecessary collection or unlawful use or disclosure of information.

POLICY

This policy sets out how **ds** meets its responsibilities to protect privacy of personal and sensitive information and ensure that all **ds** understands and acts in accordance with relevant Privacy obligations and processes.

ds will be open and transparent in how it uses and manages client personal information, so that all clients can be confident that **ds** will uphold and protect their rights to privacy.

ds's role as a not-for-profit organisation, which includes its provision of health services in the state of Victoria, i.e. psycho-social mental health services for individuals, families, young people and children, and services on behalf of the Commonwealth and Victorian and local governments.

ds is therefore required to comply with each of the following:

» the Australian Privacy Principles, as set out in the Commonwealth Privacy Act 1988

» the Information Privacy Principles, as set out in the Privacy and Data Protection Act 2014 (Vic)

» the Health Privacy Principles, as set out in the Health Records Act 2001 (Vic)

PROCEDURE

In the delivery of providing programs and services, personal and sensitive information is collected, held and maintained by **drummond street services**. **The protection and care of personal information both clients and staff is of the utmost priority.**

All IT platforms, systems and processes, as well as our individual and collective behaviours and practices is critical in ensuring that all personal, sensitive information, and that which can identify a person is collected, handled, stored, used and shared legally, appropriate, and only with:

- **informed consent of the individual** (except where legally required; including;
- protecting individuals, children and members of public from harm,
- **family violence information-sharing purposes,**
- **subpoena**
- **FOI requests, access to individual clients records and where no breach of another person's information**

All staff, including contractors, students, volunteers must ensure they are aware of their privacy obligations, and well as the organisation's privacy controls to ensure safety of personal and sensitive information.

drummond street services complies with all the relevant Acts which govern the collection, use, disclosure, quality, security and disposal of personal health information and provide people with a legally enforceable right of access and correction of the health information held about them. Both Acts provide for the right for a person to make, and process by which a person makes, a complaint if they believe their personal information has been mishandled.

ds will adhere to the following processes for managing client privacy, which are further explained below:

1. **ds** privacy policies are clearly expressed and up to date
2. **ds** will only collect personal and sensitive information when it is relevant
3. **ds** will only collect personal and sensitive information with consent and in a fair way
4. Notification
5. Use and disclosure
6. Access
7. Correction
8. Data security
9. Data quality
10. Government related identifiers
11. Cross border transfer of data
12. Retention of personal information
13. Disposal
14. Transfer
15. Anonymity and pseudonymity
16. Unsolicited information
17. Direct marketing
18. Data breaches
19. Physical privacy
20. Complaints

1 ds privacy policy and information will be clearly expressed, accessible and current

ds clearly expresses its Privacy policies and processes and how **ds** manages personal information. It will also outline how an individual may obtain access to their information that supports transparency, accountability, duty of care and safety. In addition to ensuring the organisation's compliance, at all times and reflects current privacy law and regulations.

Privacy information must be available to clients and available on all ds and sub-entities websites.

At reception, **ds** will display posters, brochures and factsheets on privacy so that clients can be informed of their rights and be reassured on how **ds** will manage and protect their personal information.

2 ds will only collect personal and sensitive information when it is relevant

ds collects only information that is relevant for the services it offers. **ds** will collect and hold both personal information, and where required, sensitive information, only if it is reasonably needed to provide services. Any caveats or processes relating to privacy or sharing of personal and sensitive information will be clearly given or an included on any forms and outlined as part of client information i.e. **Client *Rights and Responsibilities* information**. This information should be available in accessible languages, including community languages and support people of all abilities and background with this information to ensure informed consent.

Personal information that **ds** will collect, and hold covers items such as:

- Name
- Title
- Gender
- Address
- Contact information

Sensitive information that **ds** may collect, and hold covers items such as:

- Health information, including both physical health and mental health
- Racial or ethnic origin
- Sexual orientation

3 **ds** will only collect personal and sensitive information with consent and in a fair and transparent way

ds will only collect information using lawful and fair means and will do so in a way that is not unreasonable or intrusive and with consent.

ds will only collect information about an individual client directly from that client wherever it is reasonable and practicable to do so, unless the client gives permission to collect that information from someone other than themselves (e.g. parent or carer or third party such as another support service or relevant organisation), or **ds** is required to by law.

It is essential that all staff understand and comply with relevant policies relating to client information including ds Informed Consent Policy.

4 Notification

Whenever **ds** collects personal information, or as soon as practicable, **ds** will inform the individual client of:

- Contact details of our organisation, and the sub-entity (i.e. queerspace, the drum, CFRE, Stepfamilies Australia – all services and programs that **ds** has the legal obligation for) and that is requiring the specific information or collecting it, i.e. support services, funder and contractual information or research and evaluation purposes.
- what information and the process for an individual to gain access to their information
- the purposes for which the information is collected
- what scope and limits relating to who and where information is shared (e.g. (the types of individuals or organisations to which) **ds** usually discloses information of that kind
- any law that requires the particular information to be collected
- the main consequences (if any) for the individual if all or part of the information is not provided

5 Use and disclosure

ds will **only** use personal information for the purposes that were stated when **ds** first collected it, unless:

- the client consents to allow **ds** to use the information for a different purpose
- **ds** reasonably believe that use or disclosure is necessary to lessen or prevent
  - *(i)* a serious threat to an individual's life, health, safety or welfare; or
  - *(ii)* a serious threat to public health, public safety or public welfare
- **ds** is required to, or reasonably believes that it is required to, disclose by law, in which case **ds** will keep a record of any such disclosure.
- For any other lawful purpose as a provider of mental health services as permitted in the Health Records Act 2001 (Vic)

ds will use client personal and sensitive information for research, compilation or analysis of statistics, in the public interest, so long as the information is not published in a form that identifies any particular individual. Any research or evaluation activities may also be subject to independent ethics review processes. How research and evaluation is conducted by the agency, including its ethical principles is outlined in **CFRE's Research and Evaluation strategy**.

If a client asks that **ds** provide personal health information to another health or relevant service provider or instructs another provider to make the request, ds **will provide a copy or summary of the health information and ensure a client's consent is clearly recorded and documented**.

6 Access

Whenever asked, **ds** will inform the individual whether **ds** holds personal information about them and will describe in general terms **what sort of personal information** ds **holds, for what purposes, and how** ds **collects, holds, uses and discloses that information**.

In addition, **ds** will allow individuals to have full access to their personal information that **ds** holds, unless excepted by law.

Examples of permitted exceptions include situations where:

- **ds** reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or
- giving access would have an unreasonable impact on the privacy of other individuals

In such exceptional circumstances, **ds** will endeavour to provide the client with the maximum access permitted by law.

When requested by a client to gain access to their personal information, **ds** will provide access within a reasonable time, **no later than 28 business days** effective from the date a request has been received, and in a manner that the individual client has requested where that request was reasonable.

In some instances, usually related to FOI requests, **ds** may elect to charge the client for access to personal information if the gathering of information is considered unreasonable in terms of cost and resources required to generate this information. In the exceptional circumstances where a fee may be required, the client is informed in advance.

In the event that **ds** refuses to give the client access to personal information, **ds** will give written advice that includes:

- reasons for refusal unless that would be unreasonable to do so
- mechanisms available to complain about the refusal; and
- any other matter prescribed by privacy regulations.

7 Correction

ds staff will take all reasonable steps to ensure that personal information it holds about an individual is accurate, up to date, complete, relevant and not misleading. Whenever an individual requests **ds** to correct the information, **ds** will take reasonable steps to do so. **ds** will also proactively correct personal information if it is satisfied that it is inaccurate, out of date, incomplete, irrelevant or misleading. *Refer to Case Notes Policy*.

If **ds** has previously disclosed this information to another organisation, then:

- **ds** will take reasonable steps to notify any health service or other relevant service providers to whom **ds** disclosed the information before its correction and who may reasonably be expected to rely on that information in the future.
- For all other organisations, **ds** will take reasonable steps to notify the correction when requested by the individual client unless impractical or unlawful to do so.

ds will respond within a reasonable period to any request made by a client to correct personal information, and in any event within 28 days of receiving the request.

Any changes to client record should be noted with a visible and apparent audit trail.

- Changes and inclusions in the client record should clearly denote which practitioner or staff member made any changes and the date and record clearly in a case note
- Note any comments on incorrect information on a case record and ensure any historical inaccuracies are not used in an ongoing capacity and restricted.

- Client information is required to be accurate and lawful, so it important to make amendments but it is also unlawful to delete or destroy client records. Please seek advice before any actions.

In the event that the corrections required are complex or numerous which may confuse or cause an error in relation to its interpretation, only then would a new client record be created, and be linked or where appropriate archived.

If **ds** and the individual disagree about whether the information is accurate, and the individual requests the entity to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, **ds** will take reasonable steps to make that statement apparent to users of the information.

8 Data security

ds will take all reasonable step to protect a client's personal information from

misuse, interference and loss, and from unauthorised access, modification or disclosure.

ds will primarily store client information on the **ds Client Record Management system**, which has appropriate and reasonable controls, including user access controls and security features All information is stored digitally, with cloud hosting in Australia, that is obliged to safeguard and ensure their compliance with privacy laws. **ds**'s current CRM hosted by a Perth data centre.

In addition, **ds** may also have certain client records which it retains in physical form. **ds** has specific controls in place to ensure that hard copies and electronic copies of client records are protected from unauthorised access.

CRM – Internal controls:

- Password protected access,
- regular password change policy,
- independent system login credentials,
- limited number of system administrators,
- restrictions in user permissions dependent upon job function,
- regular audits of active user accounts by system administrators.

Vendor Controls:

- Limited number of system administrators,
- hashing of sensitive information in restricted testing environment.

Storage Controls:

- Hosting is on Australian servers with ISO 27001, ISO 9001,
- Uptime Institute Tier III certification.
- Physical and digital security systems and protocols, with multi-layered access authentication.

Client Records and Information

All client records are Agency records and must be maintained and stored under conditions which ensure the strictest confidentiality and privacy. Terminated case records (hard copy files) are archived with in an off-site specialist, Archival Facility **for a period up to 7 years in accordance with Commonwealth Archival requirements, or in the case of children up to 30 years**. Any permissions to access historical or archival files is on a case-by-case basis and only with approval by Executive or General Manager, which each request recorded. All client's files are archived and securely stored off-site at Iron Mountain – Secure Archival specialists.

- Client information that identifies an individual – hard copy records must be stored in locked filing cabinets which **ALWAYS** should be located away from public areas and out of the sight of clients. This applies to all **ds** locations.
- Files and computer printouts **must not** be left on or in desks when unattended. This constitutes a serious Privacy breach.
- **No** client information is to be left in Reception, counselling areas or meeting or training rooms when unattended.
- Access to records or personal, sensitive information should be limited to as few personnel as necessary within the Agency. This includes emails, faxes, databases. If there is client information in an email it should only be sent to the relevant staff members for the purpose of providing services. (see *Administration* and *Programs Policies and Procedures Manuals* including the

- Additional client information including practitioner's diaries or Registers should be locked away and not accessible or left unattended.

Client Records are the property of the Agency and must not be removed from Agency premises unless specified permission is sought from the Executive and safety is maintained.
(See ds Client Case-Files and Case-Notes Policy).

HR/Staff Records

All personal information collected in the course of a **ds** staff member's employment is held in their Personnel File and located in a locked filing cabinet within the HR Managers office. Electronic records are also stored on **ds** Intranet, with password protected and restricted access based on function, role and need to know basis. Only the CEO, HR Manager, Line Managers and Systems Administrators are able to access those files. This also includes case practice supervision notes. In addition, each staff member's Supervision File is located with their Line Manager in a locked filing cabinet.

9 Data quality

All **ds** staff will take all reasonable steps to ensure that the personal information **ds** collects is accurate, up to date, complete, and relevant for how the purposes the information is used.

10 Adoption, use or disclosure of government related identifiers

ds will assign identifiers to individual clients only when reasonably necessary to deliver service. Unless specifically required to do so by Australian law, **ds** will ensure that this client identifier does not match or correspond to any government related identifier for that individual.

ds will not ask clients to provide a unique government identifier to obtain a service unless that is required by law or is directly related to the service.

ds will also not use or disclose the government related identifier of an individual, except to verify the identity of the individual, or to meets its legal obligations.

11 Cross border transfer of data

ds assesses that it is unlikely that **ds** would transfer client data outside of Australia. **ds**'s holding, management and processing of client data remains within the state of Victoria and transfer's data to third parties or contractors in Western Australia (CRM data) and ACT (DEX Department of Social Services Data Exchange for specific program and client data) outside of Victoria except in the following circumstances:

ds will only transfer client personal data to organisations outside of Victoria, and within Australia, if one on the following applies:

a. **ds** reasonably believes that the recipient of the information is legally bound by the same privacy principles as **ds** is under Victorian law and the relevant Commonwealth laws; or

b. the individual consents to the transfer; or

c. the transfer is necessary for the performance of a contract between the individual and the organisation; or

d. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between **ds** and a third party; or

e. the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Information Privacy Principles.

f. the transfer is authorised or required by any other Australian law; or

g. all of the following apply:

(i) the transfer is for the benefit of the individual;

(ii) it is impracticable to obtain the consent of the individual to that transfer;

(iii) if it were practicable to obtain that consent, the individual would be likely to give it

(iv) Outside Australia

ds will only transfer data to third party organisations or individuals outside of Australia if all of the above restrictions apply, and in addition that:

- **ds** has taken reasonable steps to ensure that the overseas recipient does not breach Australian privacy law, and
- before the client gives consent, **ds** informs the client that data may be transferred outside of Australia, and the client maintains their consent
- or, if the transfer is required by Australian law

12 Retention of personal information

Under Victorian law, **ds** retains client personal information as follows:

(i) in the case of information collected while the individual was a child, until the individual attains the age of 25 years; or

(ii) in any case, until 7 years after the last occasion on which a health service was provided to the individual whichever is the later.

Subject to those requirements, **ds** will only hold client information for the purposes of providing services. Client records should be closed if they are no longer receiving a service, or there is no longer any duty to disclose to a third party under the law and there clearly not a requirement to hold information under the Australian law. unless it is Any client record that remains open should have clear reasons recorded on the individual file.

13 Disposal

All records as a result of the work of all **ds** programs and sub-entities are employer records and must not be deleted or destroyed. **It is a serious breach if a ds staff member does this without any explicit authority.** No member of **ds** staff will delete or destroy client personal information **unless and until** it is lawful to do so.

When **ds** deletes or destroy client records:

- » All reasonable steps must be made to ensure that information is de-identified or permanently destroyed to minimise any risks of personal, sensitive information being available and disposed of via security bins or digitally erased and removed from data backups within a reasonable timeframe.
- » **ds** will retain a written record of the name of the individual to whom the health information related, the period covered by it and the date on which it was deleted in case note.

14 Transfer

When **ds** permanently transfers client information to another organisation, **ds** will note of the individual and/or organisation information in case notes before it is closed.

In the event of closure of practice, **ds** will follow in full the process set out in Health Privacy Principle 10. **(https://www2.health.vic.gov.au/mental-health/rights-and-advocacy/privacy/rights-and-privacy-principles)**

15 Anonymity and pseudonymity

Wherever it is lawful and practicable, individuals have the option of not identifying themselves by their formal legal name when dealing with **ds**. Those who do not want to identify themselves do need to be informed of the limits of services provided without relevant information.

16 Unsolicited information

In situations where a **ds** staff member receives personal information, but did not ask for it, as soon as practicable, it must be determined, whether it would have most likely collected the information as part of the **ds** services? If not, as soon as practicable, but only if it is lawful and reasonable to do so, **ds** will destroy the information or ensure that the information is de-identified.

If an individual client gives **ds** information in confidence about someone else and requests that the information is not communicated to that individual, then **ds** will

- confirm that the information is to remain confidential
- retain that information only if it relevant for the care of the individual
- take reasonable steps to ensure that the information is accurate and not misleading, and
- record that the information is given in confidence and is to remain confidential.

17 Direct marketing

ds will not use personal or sensitive information about an individual for the purposes of direct marketing unless it has the consent of the individual. Any consents must be clearly recorded in client records, this includes any promotion of **ds** and other services.

Individuals should be able to withdraw their consent to have their data used for direct marketing or receiving of information as easy as possible.

18 Notifiable Data Breaches

ds has a legal responsibility to report privacy breaches under the *Notifiable Data Breaches regulations*. Under the **scheme**, an organisation or agency must comply with Australian privacy law if it is likely to cause you serious harm.

Examples of serious harm include:

- identity theft
- financial loss through fraud
- a likely risk of physical harm, such as by an abusive ex-partner
- serious psychological harm
- serious harm to an individual's reputation, and;

ds will need to carry out an assessment when there is a reasonable belief there may have been:

- serious data or information loss;
- unauthorised access to, or,
- unauthorised disclosure of personal information

ds has 30 days to assess whether a data breach is likely to result in serious harm.

When a data breach occurs, **ds** must mitigate and deploy measures or actions to reduce the chances of harm to the individual/s. If these measures are successful, and the data breach is not likely to result in serious harm, the organisation is not required to report to the Office of the Australian Information Commission (OIAC) individual about the data breach. Refer to **https://www.oaic.gov.au/privacy/data-breaches/what-is-a-notifiable-data-breach/** for further information.

A serious data breach must also be reported as **ds Critical Incident** and may also have to be reported to the relevant funder as part of their **Incident Reporting and Management processes**. Therefore, any serious breaches must be escalated to Senior Managers as soon as possible.

19 Physical privacy

As well as privacy of data, **ds** will ensure that the privacy of clients when visiting **ds** sites is protected, including their personal and sensitive information is protected from unauthorised disclosure, and ensuring appropriate levels of privacy in reception areas, shared areas, counselling rooms and training or group settings.

20 Privacy complaints

If an individual client is concerned about how ds is managing their privacy, the individual should make a complaint to the **ds** Chief Executive Officer. A breach of privacy is a serious matter and the organisation must adhere to it **ds Complaints Policy as well as ds Incident Management Policy and Procedures**. The ds Chief Executive Officer will review and investigate the complaint, and provide a written response to the client within 30 days setting out:

- **ds**' response to the complaint, unless that would be unreasonable or unlawful to do so
- the mechanisms available to complain about **ds**' response

Clients may also complain to:

Office of the Australian Information Commissioner

GPO Box 5218
Sydney NSW 2001

https://www.oaic.gov.au/individuals/how-do-i-make-a-privacy-complaint

Office of the Victorian Information Commissioner

Tel: 1300 00 6842

Email: privacy@ovic.vic.gov.au

https://ovic.vic.gov.au/resource/privacy-complaints-at-ovic-guide-for-individuals/

Health Complaints Commissioner

Tel: 1300 582 113

Level 26
570 Bourke Street
Melbourne Vic 3000

https://hcc.vic.gov.au/public/about-complaints

Legislation, Regulation, Standards

Privacy Act 1988 (Cth)

Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)

Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)

Privacy and Data Protection Act 2014 (Vic)

Health Records Act 2001 (Vic)

National Standards for Mental Health Services 2010

QIC Health and Community Services Standards 7th Edition 2017

Human Services Standards

drummond street services
wellbeing for life

Stepfamilies Australia
Strengthening Stepfamilies

queerspace
our health in our hands

CFRE
Centre for FAMILY RESEARCH and EVALUATION

the drum
YOUTH SERVICES

We acknowledge the traditional owners of the land where we work and pay respects to elders past, present and future.